BSI VDM-SL Type Model and Proof Theory

Roger Bishop Jones
ICL Defence Systems

This document consists of overheads for introducing the discussion of the VDM panel (technical subgroup) on the above topic.
1. SOME RELEVANT DOCUMENTS

A Type Model for VDM - Brian Monahan

Notes on VDM Type Model - Roger Jones

Kentrikos - Havelund & Wagner

Notes on Kentrikos - Roger Jones

Plan for VDM-SL Proof Theory - Roger Jones

Naive Denotational Semantics - Blikle & Tarleki

A Semantics of Multiple Inheritance - Cardelli

UST in SML, LPF in SML - Roger Jones
2. PRIMARY ISSUES (from proof-theoretic viewpoint)

REFLEXIVE DOMAINS

TYPE INHERITANCE

FUNCTIONS SPACES
(continuity, strictness)

STRATIFICATION
(1, 2 or 3 layers)

When do we need to have these issues settled?
3. DIFFICULTIES WITH BQM MODEL

Is it 2 or 3 layers?
(and why)

How does the record type constructor work
(proof of closure please)

Quantification and Continuity

4. CONTINUITY

Identifying FORMULAE with
CONTINUOUS BOOLEAN EXPRESSIONS

gives a logic with
NEGLIGIBLE expressive power.

QUANTIFICATION is NOT CONTINUOUS.

IMPLICATION is NOT MONOTONIC (or strict).

In the VDM RL semantics, specifications
which ought to denote discontinuous functions
simply fail to have models, they are inconsistent.
5. WHAT FUNCTION SPACE IS BEST?

SCOTT CONTINUOUS?
No, continuity is too strong a constraint.
(for a specification language)

BLIKLE/Z PARTIAL FUNCTION SPACE.
\[(A \text{ pf } B) = A \times B = \{ r \mid r \subseteq P(A \times B) \land r \text{ is many-one} \} \]
No, strictness is too strong a constraint.

KENTRIKOS PARTIAL FUNCTION SPACE
No, it doesn’t admit closure.
(a little overpopulated)

ADD BOTTOMS and use TOTAL FUNCTIONS?
\[(A \text{ pf } B) = (A+) \rightarrow (B+) \]

RBJ PF SPACE?
\[(A \text{ pf } B) = (A + \emptyset) \times (B - \emptyset) \]